CLAIMS

We claim:

1. A computer implemented method for updating a current security scheme on a computer system, said computer implemented method comprising the steps of:

(a) receiving log-in data for a client during a first log-in attempt;

(b) authenticating said client, wherein said step (b) includes the steps of:

(1) applying a first function to a value in said log-in data to obtain a first result, and

(2) employing said first result in determining whether to authenticate said client during said first log-in attempt;

(c) determining that said current security scheme is to be replaced by a desired security scheme; and

(d) modifying at least one record in said computer system in response to said step (c), wherein said step (d) includes the step of:

(1) applying a second function to said value received in said step (a) to obtain a second result.

2. The computer implemented method of claim 1, wherein said computer system maintains a log-in record, wherein said step (b)(2) includes the steps of:

(i) comparing said first result obtained in said step (b)(1) to a first value stored in said log-in record.

3. The computer implemented method of claim 2, wherein said step (d) includes the step of:

(2) replacing said first value in said log-in record with said second result obtained in said step (d)(1).

4. The computer implemented method of claim 3, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function.

5. The computer implemented method of claim 2, wherein said step (b) includes the steps of:

(3) applying a third function to said value in said log-in data to obtain a first credential; and

(4) decrypting a third value in said log-in record to obtain a decrypted value, wherein said step (b)(4) employs said first credential.

6. The computer implemented method of claim 5, wherein said step (b) further includes the step of:

(5) forwarding said decrypted value to a primary computer system.

7. The computer implemented method of claim 5, wherein said step (d) includes the steps of:

(2) replacing said first value in said log-in record with said second result obtained in said step (d)(1);

(3) applying a fourth function to said value in said log-in record to obtain a second credential;

(4) encrypting a quantity to obtain a fourth value, wherein said step (d)(4) employs said second credential; and

(5) replacing said third value in said log-in record with said fourth value.

8. The computer implemented method of claim 7, wherein:

said first function is a first hash function and said second function is a second hash function different than said first hash function, and

said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function.

9. The computer implemented method of claim 2, wherein said step (b) includes the steps of:

(3) inputting said value in said log-in data into a first cryptographic cipher to obtain a first encryption key; and

(4) decrypting a third value in said log-in record to obtain a decrypted value, wherein said step (b)(4) employs said first encryption key.

10. The computer implemented method of claim 9, wherein said step (b) further includes the step of:

(5) forwarding said decrypted value to a primary computer system.

11. The computer implemented method of claim 9, wherein said step (d) includes the steps of:

(2) replacing said first value in said log-in record with said second result obtained in said step (d)(1);

(3) inputting said value in said log-in data into a second cryptographic cipher to obtain a second encryption key;

(4) encrypting a quantity to obtain a fourth value, wherein said step (d)(4) employs said second encryption key; and

(5) replacing said third value in said log-in record with said fourth value.

12. The computer implemented method of claim 1, wherein said computer system maintains a log-in record, wherein said step (b)(2) includes the steps of:

(i) decrypting a first value in said log-in record to obtain a decrypted value, wherein said step (b)(2)(i) employs said first result as a decryption key; and

(ii) forwarding said decrypted value to a primary computer system.

13. The computer implemented method of claim 12, wherein said step (d) includes the steps of:

(2) encrypting a quantity to obtain a second value, wherein said step (d)(3) employs said second result obtained in said step (d)(1); and

(3) replacing said first value in said log-in record with said second value.

14. The computer implemented method of claim 13, wherein:

said first function is a first hash function and said second function is a second hash function different than said first hash function, and

said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function.

15. The computer implemented method of claim 11, wherein:

said first function is a first cryptographic cipher and said second function is a second cryptographic cipher different than said first cryptographic cipher, and

said third function is a third cryptographic cipher and said fourth function is a fourth cryptographic cipher different than said third cryptographic cipher.

16. The computer implemented method of claim 1, further including the steps of:

(e) receiving log-in data for said client during a second log-in attempt;

(f) authenticating said client during said second log-in attempt, wherein said step (f) includes the steps of:

(1) applying said second function to a value in said log-in data received in said step (e) to obtain a third result, and

(2) employing said third result in determining whether to authenticate said client during said second log-in attempt.

17. The computer implemented method of claim 1, wherein said computer system includes a log-in record corresponding to said client, wherein said log-in record includes a first entry identifying said current security scheme, said computer implemented method further including the step of:

(g) replacing said first entry in said log-in record with a second entry identifying said desired security scheme.

18. A computer implemented method for providing a client with access to a primary system through an intermediate system, said computer implemented method comprising the steps of:

(a) creating a log-in record, wherein said log-in record includes a security identifier and a first encrypted value, wherein said security identifier corresponds to a current security scheme employed by said intermediate system;

(b) receiving log-in data for said client;

(c) authenticating access of said client to said intermediate system, based on data from said log-in data and data from said log-in record;

(d) obtaining authentication data to send to said primary system, wherein said authentication data includes data from a decrypted version of said first encrypted value;

(e) determining that said current security scheme is to be replaced by a desired security scheme; and

(f) modifying said log-in record, wherein said step (f) includes the steps of:

(1) updating said security identifier to correspond to said desired security scheme,

(2) employing data in said log-in data received in said step (b) to calculate a second encrypted value, and

(3) replacing said first encrypted value with said second encrypted value.

19. The computer implemented method of claim 18, wherein said step (c) includes the steps of:

(1) applying a first function to a value in said log-in data to obtain a first result, and

(2) comparing said first result obtained in said step (c)(1) to a first value stored in said log-in record.

20. The computer implemented method of claim 19, wherein said step (f) includes the steps of:

(4) applying a second function to said value in said log-in data to obtain a second result; and

(5) replacing said first value in said log-in record with said second result obtained in said step (d)(4).

21. The computer implemented method of claim 20, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function.

22. The computer implemented method of claim 20, wherein said step (d) includes the steps of:

(3) applying a third function to said value in said log-in data to obtain a first credential; and

(4) decrypting said first encrypted value in said log-in record to obtain a first decrypted value, wherein said step (d)(4) employs said first credential, wherein said authentication data includes said first decrypted value.

23. The computer implemented method of claim 22,

wherein said step (f)(2) includes the steps of:

(i) applying a fourth function to said value in said log-in record to obtain a second credential; and

(ii) encrypting a quantity to obtain said second encrypted value, wherein said step (f)(2)(ii) employs said second credential.

24. The computer implemented method of claim 23, wherein said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function.

25. The computer implemented method of claim 20, wherein said step (d) includes the steps of:

(3) inputting said value in said log-in data to a first cryptographic cipher to obtain a first decryption key; and

(4) decrypting said first encrypted value in said log-in record to obtain a first decrypted value, wherein said step (d)(4) employs said first decryption key, wherein said authentication data includes said first decrypted value.

26. The computer implemented method of claim 25,

wherein said step (f)(2) includes the steps of:

(i) inputting said value in said log-in record to a second cryptographic cipher to obtain said second encryption key;

(ii) encrypting a quantity to obtain said second encrypted value, wherein said step (f)(2)(ii) employs said second encryption key.

27. The computer implemented method of claim 18, wherein said step (d) includes the steps of:

(1) applying a first function to a value in said log-in data to obtain a first credential; and

(2) decrypting said first encrypted value in said log-in record to obtain a first decrypted value, wherein said step (d)(2) employs said first credential, wherein said authentication data includes said first decrypted value.

28. The computer implemented method of claim 27,

wherein said step (f)(2) includes the steps of:

(i) applying a second function to said value in said log-in record to obtain a second credential; and

(ii) encrypting a quantity to obtain said second encrypted value, wherein said step (f)(2)(ii) employs said second credential.

29. The computer implemented method of claim 28, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function.

30. The computer implemented method of claim 28, wherein said first function is a first cryptographic cipher and said second function is a second cryptographic cipher different than said first cryptographic cipher.

31. A processor readable storage medium having processor readable code embodied on said processor readable storage medium, said processor readable code for programming a processor to perform a method for updating a current security scheme on a computer system, said method comprising the steps of:

(a) receiving log-in data for a client during a first log-in attempt;

(b) authenticating said client, wherein said step (b) includes the steps of:

(1) applying a first function to a value in said log-in data to obtain a first result, and

(2) employing said first result in determining whether to authenticate said client during said first log-in attempt;

(c) determining that said current security scheme is to be replaced by a desired security scheme; and

(d) modifying at least one record in said computer system in response to said step (c), wherein said step (d) includes the step of:

(1) applying a second function to said value received in said step (a) to obtain a second result.

32. The processor readable storage medium of claim 31, wherein said computer system maintains a log-in record, wherein said step (b)(2) includes the steps of:

(i) comparing said first result obtained in said step (b)(1) to a first value stored in said log-in record, and

wherein said step (d) includes the step of:

(2) replacing said first value in said log-in record with said second result obtained in said step (d)(1).

33. The processor readable storage medium of claim 32, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function.

34. The processor readable storage medium of claim 32, wherein said step (b) includes the steps of:

(3) applying a third function to said value in said log-in data to obtain a first credential; and

(4) decrypting a third value in said log-in record to obtain a decrypted value, wherein said step (b)(4) employs said first credential, and

wherein said step (d) includes the steps of:

(3) applying a fourth function to said value in said log-in record to obtain a second credential;

(4) encrypting a quantity to obtain a fourth value, wherein said step (d)(4) employs said second credential; and

(5) replacing said third value in said log-in record with said fourth value.

35. The processor readable storage medium of claim 34, wherein:

said first function is a first hash function and said second function is a second hash function different than said first hash function, and

said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function.

36. The processor readable storage medium of claim 32, wherein said step (b) includes the steps of:

(3) inputting said value in said log-in data into a first cryptographic cipher to obtain a first encryption key; and

(4) decrypting a third value in said log-in record to obtain a decrypted value, wherein said step (b)(4) employs said first encryption key, and

wherein said step (d) includes the steps of:

(3) inputting said value in said log-in data into a second cryptographic cipher to obtain a second encryption key;

(4) encrypting a quantity to obtain a fourth value, wherein said step (d)(4) employs said second encryption key; and

(5) replacing said third value in said log-in record with said fourth value.

37. The processor readable storage medium of claim 31, wherein said computer system maintains a log-in record, wherein said step (b)(2) includes the steps of:

(i) decrypting a first value in said log-in record to obtain a decrypted value, wherein said step (b)(2)(i) employs said first result as a decryption key; and

(ii) forwarding said decrypted value to a primary computer system, and

wherein said step (d) includes the steps of:

(2) encrypting a quantity to obtain a second value, wherein said step (d)(2) employs said second result obtained in said step (d)(1); and

(3) replacing said first value in said log-in record with said second value.

38. The processor readable storage medium of claim 37, wherein:

said first function is a first hash function and said second function is a second hash function different than said first hash function, and

said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function.

39. The processor readable storage medium of claim 37, wherein:

said first function is a first cryptographic cipher and said second function is a second cryptographic cipher different than said first cryptographic cipher, and

said third function is a third cryptographic cipher and said fourth function is a fourth cryptographic cipher different than said third cryptographic cipher.

40. The processor readable storage medium of claim 31, wherein said computer system includes a log-in record corresponding to said client, wherein said log-in record includes a first entry identifying said current security scheme, said computer implemented method further including the step of:

(e) replacing said first entry in said log-in record with a second entry identifying said desired security scheme.

41. A processor readable storage medium having processor readable code embodied on said processor readable storage medium, said processor readable code for programming a processor to perform a method for providing a client with access to a primary system through an intermediate system, said method comprising the steps of:

(a) creating a log-in record, wherein said log-in record includes a security identifier and a first encrypted value, wherein said security identifier corresponds to a current security scheme employed by said intermediate system;

(b) receiving log-in data for said client;

(c) authenticating access of said client to said intermediate system, based on data from said log-in data and data from said log-in record;

(d) obtaining authentication data to send to said primary system, wherein said authentication data includes data from a decrypted version of said first encrypted value;

(e) determining that said current security scheme is to be replaced by a desired security scheme; and

(f) modifying said log-in record, wherein said step (f) includes the steps of:

(1) updating said security identifier to correspond to said desired security scheme,

(2) employing data in said log-in data received in said step (b) to calculate a second encrypted value, and

(3) replacing said first encrypted value with said second encrypted value.

42. The processor readable storage medium of claim 41, wherein said step (c) includes the steps of:

(1) applying a first function to a value in said log-in data to obtain a first result, and

(2) comparing said first result obtained in said step (c)(1) to a first value stored in said log-in record, and

wherein said step (f) includes the steps of:

(4) applying a second function to said value in said log-in data to obtain a second result; and

(5) replacing said first value in said log-in record with said second result obtained in said step (d)(4).

43. The processor readable storage medium of claim 42, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function.

44. The processor readable storage medium of claim 42, wherein said step (d) includes the steps of:

(3) applying a third function to said value in said log-in data to obtain a first credential; and

(4) decrypting said first encrypted value in said log-in record to obtain a first decrypted value, wherein said step (d)(4) employs said first credential, wherein said authentication data includes said first decrypted value, and

wherein said step (f)(2) includes the steps of:

(i) applying a fourth function to said value in said log-in record to obtain a second credential; and

(ii) encrypting a quantity to obtain said second encrypted value, wherein said step (f)(2)(ii) employs said second credential.

45. The processor readable storage medium of claim 42, wherein said step (d) includes the steps of:

(3) inputting said value in said log-in data to a first cryptographic cipher to obtain a first decryption key; and

(4) decrypting said first encrypted value in said log-in record to obtain a first decrypted value, wherein said step (d)(4) employs said first decryption key, wherein said authentication data includes said first decrypted value, and

wherein said step (f)(2) includes the steps of:

(i) inputting said value in said log-in record to a second cryptographic cipher to obtain said second encryption key;

(ii) encrypting a quantity to obtain said second encrypted value, wherein said step (f)(2)(ii) employs said second encryption key.

46. The processor readable storage medium of claim 41, wherein said step (d) includes the steps of:

(1) applying a first function to a value in said log-in data to obtain a first credential; and

(2) decrypting said first encrypted value in said log-in record to obtain a first decrypted value, wherein said step (d)(2) employs said first credential, wherein said authentication data includes said first decrypted value, and

wherein said step (f)(2) includes the steps of:

(i) applying a second function to said value in said log-in record to obtain a second credential; and

(ii) encrypting a quantity to obtain said second encrypted value, wherein said step (f)(2)(ii) employs said second credential.

47. The processor readable storage medium of claim 46, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function.

48. The processor readable storage medium of claim 46, wherein said first function is a first cryptographic cipher and said second function is a second cryptographic cipher different than said first cryptographic cipher.

49. An apparatus providing a client with access to a primary system through an intermediate system, said apparatus comprising:

a processor; and

a processor readable storage medium, in communication with said processor, said processor readable storage medium storing code for programming said processor to perform a method for updating a current security scheme on a computer system, wherein said method includes the steps of:

(a) receiving log-in data for a client during a first log-in attempt;

(b) authenticating said client, wherein said step (b) includes the steps of:

(1) applying a first function to a value in said log-in data to obtain a first result, and

(2) employing said first result in determining whether to authenticate said client during said first log-in attempt;

(c) determining that said current security scheme is to be replaced by a desired security scheme; and

(d) modifying at least one record in said computer system in response to said step (c), wherein said step (d) includes the step of:

(1) applying a second function to said value received in said step (a) to obtain a second result.

50. The apparatus of claim 49, wherein said computer system maintains a log-in record, wherein said step (b)(2) includes the steps of:

(i) comparing said first result obtained in said step (b)(1) to a first value stored in said log-in record, and

wherein said step (d) includes the step of:

(2) replacing said first value in said log-in record with said second result obtained in said step (d)(1).

51. The apparatus of claim 50, wherein said step (b) includes the steps of:

(3) applying a third function to said value in said log-in data to obtain a first credential; and

(4) decrypting a third value in said log-in record to obtain a decrypted value, wherein said step (b)(4) employs said first credential, and

wherein said step (d) includes the steps of:

(3) applying a fourth function to said value in said log-in record to obtain a second credential;

(4) encrypting a quantity to obtain a fourth value, wherein said step (d)(4) employs said second credential; and

(5) replacing said third value in said log-in record with said fourth value.

52. The apparatus of claim 51, wherein:

said first function is a first hash function and said second function is a second hash function different than said first hash function, and

said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function.

53. The apparatus of claim 50, wherein said step (b) includes the steps of:

(3) inputting said value in said log-in data into a first cryptographic cipher to obtain a first encryption key; and

(4) decrypting a third value in said log-in record to obtain a decrypted value, wherein said step (b)(4) employs said first encryption key,

wherein said step (d) includes the steps of:

(3) inputting said value in said log-in data into a second cryptographic cipher to obtain a second encryption key;

(4) encrypting a quantity to obtain a fourth value, wherein said step (d)(4) employs said second encryption key; and

(5) replacing said third value in said log-in record with said fourth value.

54. The apparatus of claim 49, wherein said computer system maintains a log-in record, wherein said step (b)(2) includes the steps of:

(i) decrypting a first value in said log-in record to obtain a decrypted value, wherein said step (b)(2)(i) employs said first result as a decryption key; and

(ii) forwarding said decrypted value to a primary computer system, and

wherein said step (d) includes the steps of:

(2) encrypting a quantity to obtain a second value, wherein said step (d)(2) employs said second result obtained in said step (d)(1); and

(3) replacing said first value in said log-in record with said second value.

55. The apparatus of claim 54, wherein:

said first function is a first hash function and said second function is a second hash function different than said first hash function, and

said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function.

56. The apparatus of claim 54, wherein:

said first function is a first cryptographic cipher and said second function is a second cryptographic cipher different than said first cryptographic cipher, and

said third function is a third cryptographic cipher and said fourth function is a fourth cryptographic cipher different than said third cryptographic cipher.

57. The apparatus of claim 49, wherein said computer system includes a log-in record corresponding to said client, wherein said log-in record includes a first entry identifying said current security scheme, said method further including the step of:

(e) replacing said first entry in said log-in record with a second entry identifying said desired security scheme.